UCID902: Uncovering nation state watering hole credential harvesting campaigns targeting human rights activists by APT threat group UCID902

By Ovi Liber

Threat Report – by Ovi Liber @ Interlab

Introduction

Since 2021, Interlab has closely been monitoring events conducted by an advanced persistent threat group we track with Unidentified Cluster ID (UCID) – **UCID902.** Based on our analysis, we conclude the attempts made by this actor demonstrate continued targeting of human rights groups and activists related to advocacy of human rights in North Korea. In addition, we are continually observing this actor utilise the compromising of legitimate business websites to host their phishing kits. We believe this to be a result of either comprising of the original website developer's infrastructure, or exploitation of the web servers themselves. We have found that the actor is a motivated, well-resourced advanced persistent threat with motivations that relate closely to those demonstrated by hostile threat groups based in North Korea. The targeted threats by this group closely align with the mission of North Korea's foreign intelligence service, Reconnaissance General Bureau (RGB). This cluster overlaps with that of ESTSecurity's cluster which they call "Kumsong 121".

It should be noted that there are many overlaps between **UCID902** and threat group "Kimsuky" in regards to TTPs, motivations and modus operandi (MO), however, at the time of writing this, we have yet to see this activity group fall into our cluster for Kimsuky.

In this report we will highlight two events from our cluster that demonstrate the activity and attack campaigns lead by **UCID902**.

- On 2023-03-17, Interlab received a sample from an NGO that supports North Korean refugees. We found that this phishing campaign used a KISA Security Notification email as a lure, synonymous with historical campaigns (example: https://www.dailynk.com/20210510-3/). In addition, the phishing page mimicked that of a Naver login page, which was hosted on a legitimate Law Firm's website, resulting in a watering hole attack. The same web server IP, hosting the Law Firm's website, was also seen mimicking a Naver login page on 2023-01-27 on a Child Education website; which we saw involved in a targeted credential harvesting campaign against a Korean University professor. Both these sites were developed by the same developer and hosted on that developer's webserver. The web developer was a company based in Seoul.
- On 2023-01-25, Interlab received a sample from an activist based in South Korea who works on North Korean human rights. This campaign used a Naver alert message as an email lure, and directed the victim to a fake Naver login page hosted on a legitimate Medical Research Institutions website, indicating a watering hole attack. The server IP of this website was also seen on three other separate watering hole attacks we tracked. All three occasions saw credential harvesting campaigns targeting victims related to the MO of UCID902. These campaigns were also hosting Naver login pages. The websites used in the watering hole attacks described above were four differing Medical Research Institutions, which all shared the same web development company and server IP address.

Understanding UCID902's credential harvesting operation

We first observed **UCID902** on 2021-07-12 delivering credential phishing campaigns to activists based in the Republic of Korea. The lures aimed to appear as Naver security alerts, prompting users to input credentials, as seen in Figure 1. From 2021 to 2023, we have seen continued efforts by **UCID902** to compromise credentials from victims with the same lures and phishing kits. These lures all are synonymous with Naver security events or similar.

Figure 1 First lure observation of UCID902 by Interlab in 2021

Throughout this time, Interlab has made direct correlations within subsequent campaigns by UCID902 between events in both infrastructure (IP addresses, domains and SMTP hosts), capabilities (phishing kit) & victimology. In addition, and most notability, the actor relies heavily on watering hole attacks by compromising legitimate organisations within Korea to host phishing pages. These organisations appear to be legitimate businesses or institutions with a diverse range of industries. However, it is not the organisations themselves that relate, but the hosting provider. Throughout our tracking, we have identified many campaigns where phishing kits were hosted on legitimate company websites indicating a compromise of the website; all of these websites, within specific time windows, were hosted by the same hosting provider or hosted IP. In recent campaigns, late 2022 to early 2023, we saw constant usage of phishing kits hosted on websites built by one specific hosting provider based in Seoul, Republic of Korea. **One notable characteristic of the phish kit we have observed is that it will verify that originating client has visited the page via a common user-agent and residential IP** – if it doesn't it will redirect to the legitimate Naver login page. As a result of this methodology, with medium to high confidence, we conclude that one of **UCID902's** attack credential comprise methodology appears as this attack path demonstrated in Figure 2 as of 2023-03-17. We would like industry partners and governmental support to validate and understand this attack method, in order to defend the human rights ecosphere from this threat actor. Because of this, we welcome and encourage industry or governmental contribution or enrichment to this intelligence.

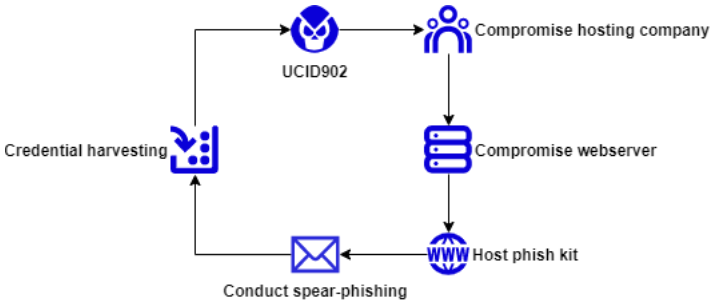

Figure 2 UCID902's credential watering hole attack pattern

Historically, we have seen more generic campaigns targeting Naver users, to which this actor's phish kits can often appear like. However, our first indication that this actor shares political and operational motivations as threat actors based in North Korea, began in early 2022. **We observed with high confidence specific infrastructure and capability correlations with a campaign targeting activists with lures masquerading as The Ministry of Unification**. This campaign included a malicious HWP document which we identified with correlations to campaigns led by APT group Kimsuky. It should be noted that this infrastructure overlap is not a common feature within our **UCID902** cluster, resulting in these specific correlations being notable findings in understanding UCID902's scope. Thus, we note that the socio-political axis of this actor closely overlaps with motivations by known threat groups based in North Korea.

Figure 3 Lure with content title as journal of South-North Korea Relation observed in 2022 targeting the same activists,
with infrastructure and capability overlap with other UCID902 credential harvesting campaigns

Due to the infrastructure, capabilities, modus operandi, victimology and other meta-features, we believe with confidence that the threat group we classify as **UCID902** are an advanced persistent threat focused on compromising credentials of activists working on North Korean human rights related activities and the unification of Korea. It should also be noted that many of the spear-phishing lures contained in campaigns led by UCID902 relate specifically to North Korean activities that would be of interest by the victims. A highly motivated actor such as this demonstrates many hallmarks of a threat group based in North Korea, however at this time we should note that we do not have

enough data points correlating to other known threat groups, such as Kimsuky, to affirm with confidence if this operation is led by them.

Figure 4 Lure by UCID902 observed targeting activist on 2023-01-25 with content title as job posting of professor position from graduate school of North Korea studies

The phish kits observed in campaigns lead by UCID902 do not appear to differ throughout our observations since 2021. Across our cluster, we have indexed DOM content of all phishing sites observed in these campaigns, resulting in all of them correlating with each other. In the phishing email, the URI (contained as a link on the green button displayed in Figure 4) contains two values that determine the targeted and the redirect. We have identified a specific encoding which the actor utilises to encode the request query parameters, which we have seen throughout campaigns lead by UCID902. When the user inputs credentials on the phish kit, we note the credentials are send in a POST request back to the comprised hosting webserver. If the originating GET request doesn't meet requirements or contain the victim identifier, the user is redirected to a different website (figure 5).

Figure 5 Example of redirection from the phishing kit when validation checks aren't valid

In addition, throughout campaigns lead by UCID902, email headers within the spear-phishing campaigns often showed the SMTP mail originating from the same infrastructure as the phishing kit and sender address containing a domain owned by the web development company.

Threat intelligence

Interlab wish to share the threat intelligence we have collected on UCID902 as soon as possible to defend and help those at risk from this actor. **We will do this once we have identified that the hosting companies we have reported to KISA are safely secured.**

If you are part of an NGO, civil society organization or other group and believe that you have been targeted by a threat actor and wish to seek help or understand more about this targeted threat, please reach out to us.

In the meantime, we will update this page with the threat intelligence we can share in due course.

Conclusion

As part of our Targeted Threats research campaign, Interlab will continue to monitor attack campaigns from hostile governments to human rights activists within Korea and across the globe. We believe **UCID902** to be an advanced persistent threat to the human rights community in Korea and will continue to monitor and support victims of this group.

We aim to support those at risk from targeted threats and share research to provide effective and actionable change to both digital security of civic organisations in Korea, East Asia and by outgrowth to global communities.

Interlab is a non-profit organization based in Seoul with a mission to create a resilient digital safety net for the freedom of citizens, providing free digital security consultations, trainings, incident response support and research of cyber threats toward civic society.

For any inquiries regarding on this report, please reach us through contact@interlab.or.kr